UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALEJANDRO MONROY, on behalf of himself and all others similarly situated,

Plaintiff,

v.

SHUTTERFLY, INC.,

Defendant.

Civil Action No.: 16-cv-10984

Hon. Joan B. Gottschall

Magistrate Judge Jeffrey T. Gilbert

REPLY IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

Lauren R. Goldman
Michael Rayfield (*pro hac vice*)
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco (*pro hac vice*)
MAYER BROWN LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

Counsel for Defendant Shutterfly, Inc.

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

ARGUMENT 3

I. BIPA DOES NOT APPLY TO SHUTTERFLY'S TECHNOLOGY 3

A. Shutterfly's Facial-Recognition Technology Obtains Only Information Derived From Photographs—Which Is Expressly Excluded Under BIPA 3

1. Plaintiff's Reading Cannot Be Squared With BIPA's Structure 3

2. Plaintiff's Reading Would Render BIPA's Exclusions Meaningless 6

B. Shutterfly's Technology Does Not Involve A "Scan Of Face Geometry" Because That Term Refers Only To An In-Person Scan 8

C. BIPA Was Never Intended To Regulate Data Derived From Online Photos 10

II. BIPA DOES NOT AND CANNOT REGULATE THE OUT-OF-STATE CONDUCT ALLEGED IN THIS CASE 12

A. Plaintiff Has Not Alleged A Sufficient Nexus To Illinois For BIPA To Apply 12

B. Applying BIPA Here Would Violate The Dormant Commerce Clause 15

III. PLAINTIFF CANNOT RECOVER UNDER BIPA BECAUSE HE HAS NOT ALLEGED ACTUAL DAMAGES 17

CONCLUSION 18

TABLE OF AUTHORITIES

Cases

Aponte v. United States,
582 F. Supp. 65 (D.P.R. 1984).....13

Avery v. State Farm Mut. Auto. Ins. Co.,
216 Ill. 2d 100 (2005) 14

Bergin v. Bd. of Trs. of Teachers' Ret. Sys.,
31 Ill. 2d 566 (1964) 12

Devoney v. Ret. Bd. of Policemen's Annuity & Ben. Fund for City of Chicago,
199 Ill. 2d 414 (2002) 6

Doe v. Chao,
540 U.S. 614 (2004).....17

Graham v. Gen. U.S. Grant Post No. 2665, V.F.W.,
43 Ill. 2d 1 (1969) 14

Gros v. Midland Credit Mgmt.,
525 F. Supp. 2d 1019 (N.D. Ill. 2007) 15

Gulf Oil Corp. v. Copp Paving Co.,
419 U.S. 186 (1974).....12

Hackett v. BMW of N. Am., LLC,
2011 WL 2647991 (N.D. Ill. June 30, 2011) 14

Healy v. Beer Inst.,
491 U.S. 324 (1989).....15

In re Facebook Biometric Info. Privacy Litig.,
185 F. Supp. 3d 1155 (N.D. Cal. 2016) 4

Jamison v. Summer Infant (USA), Inc.,
778 F. Supp. 2d 900 (N.D. Ill. 2011) 15

Laborer's Int'l Union of N. Am., Local 1280 v. State Labor Relations Bd.,
154 Ill. App. 3d 1045 (1987) 12

Landau v. CNA Fin. Corp.,
381 Ill. App. 3d 61 (2008) 2, 14

M.I.G. Invs., Inc. v. Marsala,
92 Ill. App. 3d 400 (1981) 17

McCollough v. Smarte Carte, Inc.,
2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) 18

Midwest Title Loans, Inc. v. Mills,
593 F.3d 660 (7th Cir. 2010) 16

Morley-Murphy Co. v. Zenith Elecs. Corp.,
142 F.3d 373 (7th Cir. 1998) 16

Morrison v. YTB Int'l, Inc.,
649 F.3d 533 (7th Cir. 2011) 16

Norberg v. Shutterfly, Inc.,
152 F. Supp. 3d 1103 (N.D. Ill. 2015) 4

Pace Commc'ns, Inc. v. Moonlight Design, Inc.,
31 F.3d 587 (7th Cir. 1994) 17

People v. Goossens,
39 N.E.3d 956 (Ill. 2015) 9

People v. Qualls,
365 Ill. App. 3d 1015 (2006) 8

Philips v. Bally Total Fitness Holding Corp.,
372 Ill. App. 3d 53 (2007) 14

Rivera v. Google Inc.,
2017 WL 748590 (N.D. Ill. Feb. 27, 2017) 4, 5, 6, 7, 8, 11, 12, 14, 15

Robbins v. Bd. of Trs. of Carbondale Police Pension Fund,
177 Ill. 2d 533 (1997) 7

Sam Francis Found. v. Christies, Inc.,
784 F.3d 1320 (9th Cir. 2015) (en banc) 16

Sterk v. Redbox Automated Retail, LLC,
672 F.3d 535 (7th Cir. 2012) 3, 17

T.D. v. N.Y. State Office of Mental Health,
626 N.Y.S.2d 1015 (1995) 13

Valley Air Serv. v. Southaire, Inc.,
2009 WL 1033556 (N.D. Ill. Apr. 16, 2009) 14

Vulcan Golf, LLC v. Google Inc.,
552 F. Supp. 2d 752 (N.D. Ill. 2008) 14

Walker v. S.W.I.F.T. SCRL,
491 F. Supp. 2d 781 (N.D. Ill. 2007) 14

Statutes

740 ILCS 14/5 .....10, 11

740 ILCS 14/10 .....3, 7, 9

740 ILCS 14/15 .....6, 8, 13

Other Authorities

77 Ill. Admin. Code § 697.20 13

Aleskey Golovinskiy *et al.*, *A Statistical Model for Synthesis of Detailed Facial Geometry*, COMPUTER ANIMATION AND VIRTUAL WORLDS (2011).....9

Michael Zollhofer *et al.*, *Automatic Reconstruction of Personalized Avatars from 3D Face Scans*, 25(3) ACM TRANSACTIONS ON GRAPHICS (Proc. SIGGRAPH) (July 2006) 9

Rein-Lien Hsu and Anil K. Jain, *Face Modeling for Recognition*, PROC. INT'L CONF. IMAGE PROCESSING (2001).....9

PRELIMINARY STATEMENT

Plaintiff's brief is long on breathless hyperbole and woefully short on legal analysis. Shutterfly offers a useful online tool that helps people organize and share photos of their family and friends; plaintiff characterizes it as a "tremendous, Orwellian electronic database" that presents the "greatest evil" conceivable to "reasonable expectations of privacy." BIPA is a narrow statute designed to regulate biometric-facilitated financial transactions and security screenings in Illinois; plaintiff calls it a sweeping prohibition on "the unauthorized commandeering and exploitation of one's [ ] biometric identity," the security of which is "more important" than "the security of one's social security number." Plaintiff offers little beyond rhetoric in response to the three main points in Shutterfly's motion.

First, BIPA does not cover Shutterfly's technology because the statute excludes both "photographs" and "information derived from" photographs. Plaintiff concedes (as he must) that BIPA's definition of "biometric identifier" excludes photos; that its definition of "biometric information" excludes information derived from photos; and that his case rests entirely on the allegation that Shutterfly collects and stores information derived from photos. Plaintiff nonetheless insists that because information derived from photos is not expressly excluded from the definition of *biometric identifier*, Shutterfly's facial-recognition analysis is covered under *that* provision and it was therefore required to comply with BIPA. Plaintiff still has no response, however, to our basic point: If the legislature wanted to regulate data derived from photos, there is no conceivable reason why it would have deliberately excluded this data from the definition of "biometric information." And there is a perfectly good reason why the legislature did not *also* expressly exclude such data from the definition of "biometric identifier": Derivative data is not covered by that definition in the first place, so any such exclusion would have been unnecessary.

Second, plaintiff cannot invoke BIPA because the statute does not apply extraterritorially (as he recognizes), and the complaint does not allege that "the *majority* of circumstances relating to the alleged *violation*" occurred in Illinois. *Landau*, 381 Ill. App. 3d at 65 (emphases added). Plaintiff is a Florida resident, Shutterfly is headquartered in California, and plaintiff *concedes* that his "Complaint[] fail[s] to allege that Shutterfly actually extracts scans of face geometry from photographs in Illinois"—the only BIPA "violation" alleged in the complaint. Yet plaintiff contends that he has satisfied the extraterritoriality doctrine because the person who *uploaded* his photo to Shutterfly—a third party who is not even identified in the complaint—was located in Illinois at the time and therefore "could have provided to Shutterfly a statutorily compliant written release on Plaintiff's behalf . . . in Illinois" as his "legally authorized representative."

This farfetched theory fails on multiple levels. For one thing, it is not in the complaint: Plaintiff does not allege that he and the uploader ever even met, much less that the uploader was his "legally authorized representative" within the meaning of BIPA. But in any event, the mere possibility that Shutterfly could have obtained a written release from plaintiff via an unidentified Illinois uploader cannot establish that the "majority" of relevant circumstances occurred in this State; indeed, Illinois courts have consistently held that even a *plaintiff's* Illinois residency is insufficient. Plaintiff still has not shown that Illinois has a meaningful interest in this suit.

Finally, plaintiff has claimed no "actual damages" and therefore cannot recover liquidated damages under BIPA. He argues that BIPA "entitles plaintiffs to a binary election between actual or statutory liquidated damages." That is true, but irrelevant: Under controlling precedent, liquidated damages can serve only as an "estimate of actual damages"—and where, as here, a statutory violation "results in no injury at all . . . , the only possible estimate . . . would be

zero." *Sterk*, 672 F.3d at 538. Plaintiff then argues, in a Hail Mary, that he *did* suffer actual damages—even though he neither sought nor alleged such damages in his complaint.

The Court should dismiss the complaint with prejudice.

ARGUMENT[1]

I. BIPA DOES NOT APPLY TO SHUTTERFLY'S TECHNOLOGY.

Our opening brief established that the complaint fails to state a BIPA claim because (a) the statute excludes both photographs and information derived from them; (b) Shutterfly's technology does not involve a scan of face geometry; and (c) BIPA was not intended to regulate data derived from online photos. DB 5-10. Plaintiff's responses are meritless.

A. Shutterfly's Facial-Recognition Technology Obtains Only Information Derived From Photographs—Which Is Expressly Excluded Under BIPA.

Although plaintiff acknowledges that BIPA's "definition of biometric identifiers excludes photographs," and that "[i]nformation derived from photographs is excluded from the definition of biometric information," he argues that Shutterfly's analysis of his photo constitutes a "scan of face geometry" within BIPA's definition of "biometric identifier." PB 4-5, 8-10. This reading ignores the statutory structure and would render BIPA's exclusions meaningless.

1. Plaintiff's Reading Cannot Be Squared With BIPA's Structure.

The General Assembly chose to regulate two types of biometric data: (1) original sources of information about a person ("biometric identifiers") and (2) data extracted or derived from those sources ("biometric information"). 740 ILCS 14/10. If BIPA covered data "derived from human faces depicted in photographs" (PB 4), it would be regulated as "biometric information." But as plaintiff admits, such data is expressly *excluded* from regulation under that provision. PB 5. That should end the discussion. *See* DB 6.

[1] "DB" refers to Shutterfly's opening brief. "PB" is plaintiff's opposition brief.

Plaintiff ignores the types of information that each provision *regulates*, preferring to focus myopically on what each one *expressly excludes*. He argues that "the statute explicitly excludes [ ] derivatives from the definition of biometric information, *but not* from the separate definition of biometric identifiers," and that "[t]he Court must give meaning to these significant differences in statutory language and structure." PB 8. But that is exactly what we are asking the Court to do. There is a straightforward reason why the legislature did not exclude "derivatives" from the definition of biometric identifier, or provide "a single exclusion [for] both definitions" (*id.*): The term "biometric identifier" *does not govern derivatives in the first place*; an exclusion for derivative data would have been redundant.

Consider a hypothetical statute that regulates the sale of "milk" and "milk products" to protect dairy farmers. One provision of the statute defines "milk" as "whole milk, skim milk, and cream," and excludes "soy milk, almond milk, and coconut milk." A second provision defines "milk products" as "food products derived from milk, including cheese," and excludes "food products derived from items excluded under the definition of 'milk.'" Does the statute cover soy cheese? Of course not: The statute plainly excludes all soy products. And there was no need for the statute to expressly exclude "soy cheese" from the definition of "milk," because milk (the source food) and milk products (the derivative food) are defined in separate sections.

We recognize that after our motion was filed, a court in this District rejected this same basic structural argument in denying a motion to dismiss a BIPA claim against Google. *See Rivera v. Google Inc.*, 2017 WL 748590, at *6-7 (N.D. Ill. Feb. 27, 2017).[2] The *Rivera* court made two points on this issue.

[2] As we anticipated (DB 9-10), plaintiff cites two other district court cases that denied motions to dismiss BIPA claims (PB 6-7). Plaintiff quotes their holdings, but largely disregards what we said about them: *Norberg*'s one-paragraph substantive analysis does not even mention BIPA's "photographs" exclusion, *see* 152 F. Supp. 3d at 1106, and *Facebook Biometric*'s

First, like plaintiff here, the *Rivera* court ascribed significance to the fact that the definition of "biometric identifier" does not exclude derivatives. It found that because "[t]he definition of 'biometric identifier' does *not* use words like 'derived from a person' . . . or 'based on an in-person scan,' whereas the definition of 'biometric information' does say that it is information 'based on' a biometric identifier," "there is no *parallel* structure to speak of." *Id.* at *6 (second emphasis added). Accordingly, the court found that it did not need to read the *exclusions* from "biometric information" into the definition of "biometric identifier." *See id.* This rationale is puzzling, because Google's argument (like ours here) was not that the definition of "biometric identifier" *incorporates* BIPA's exception for data derived from photos; it was that there was no *need* for such an exception because "biometric identifier" does not *cover* derivative data to begin with. *See id.* (describing Google's argument); p. 4 *supra*. We agree with *Rivera* that the structures of the two definitions are not parallel—which is precisely why "biometric identifier" must be limited to original sources, and "biometric information" limited to data extracted or derived from those sources.

Next, *Rivera* found that the legislature's express exclusion of information derived from photos was entitled to little weight because there is no clear pattern in the overall list of exclusions. *See id.* at *4, *7. The court explained that "Google's 'careful structure' argument . . . depends on drawing some structural meaning from the 'do not include' sentences" in the definition of biometric identifier, but that this "cannot be done" because the exclusions

limitation of BIPA's exclusions to "paper prints of photographs," 185 F. Supp. 3d at 1171, cannot be reconciled with the technologies covered as "biometric identifiers" or with the commonly understood meaning of "photograph" when BIPA was passed in 2008. *See* DB 9-10. Plaintiff responds only that *Facebook Biometric*'s "distinction . . . between 'paper prints of photographs' and 'digitized images'" was "drawn . . . in dicta." PB 6 n.2. It is no surprise that plaintiff does not embrace this distinction—it was expressly rejected in *Rivera*. *See* 2017 WL 748590, at *5 n.7 (noting that *Facebook Biometric* "dr[ew] a distinction, which this Opinion does not adopt, between digital photographs and physical photographs").

"comprise a mix of things that are true exceptions (that is, they otherwise would qualify as a biometric identifier) and others that read more like just-to-be-sure exclusions." *Id*. at *7. With respect, that is not a sound basis for dismissing the legislature's deliberate exclusion of information derived from photos in the only definition that encompasses derivative data. Indeed, the very concept of a "just-to-be-sure exclusion"—*i.e.*, an exclusion that is unnecessary but enacted "just to be sure"—is anathema to the well-established principle that a statute must be interpreted to give every term "independent effect." *Devoney v. Ret. Bd. of Policemen's Annuity & Ben. Fund for City of Chicago*, 199 Ill. 2d 414, 420 (2002). As explained in more detail next, *Rivera*'s (and plaintiff's) reading effectively removes BIPA's exclusions from the statute.

2. Plaintiff's Reading Would Render BIPA's Exclusions Meaningless.

Plaintiff offers no response to the straightforward point raised in our brief: If the General Assembly had intended to regulate data derived from photographs, it would not have expressly excluded such data from the definition of "biometric information." "Biometric identifiers" and "biometric information" are subject to the exact same regulations under BIPA; companies that obtain either "biometric identifiers or biometric information" must inform the subject, obtain a written release, and publish a written retention and destruction policy. 740 ILCS 14/15. Having gone out of its way to exclude a category of data from "biometric information," it would have been wholly illogical for the legislature to cover that data under "biometric identifier"— thereby subjecting it to the very same restrictions.

Plaintiff responds by quoting *Rivera* for the proposition that "[t]he *affirmative* definition of 'biometric information' does important work for [BIPA]; without it, private entities could evade . . . the Act's restrictions by converting a person's biometric identifier into some other piece of information, like . . . a unique number assigned to a person's biometric identifier." PB 9 (emphasis added) (quoting 2017 WL 748590, at *5). That objective, however, does not explain

the legislature's decision to *exclude* information derived from photos. In other words, plaintiff may be correct that the biometric-information provision was designed to prevent parties from circumventing BIPA by "manipulating a *biometric identifier* into a piece of information." *Id.* (emphasis added) (quoting 2017 WL 7489590, at *5). But the legislature deliberately declined to regulate the "manipulation" of items that are *not* biometric identifiers, including photos. Because plaintiff's claim rests on Shutterfly's alleged "manipulation" of photos, it is barred.

Plaintiff similarly misses the point by invoking "extrinsic definitions" of the term "biometrics." PB 10-12. Citing dictionaries and law review articles, he argues that this "term is [ ] routinely characterized by the use of enhanced tools of measurement and analysis made possible by modern computing technology," and that "biometric identifier" should be read with similar generality. PB 10. But BIPA does not use the term "biometrics"; it uses the term "biometric identifier" and provides its *own* definition of that term, which therefore "must be construed according to the definitions contained in the act." *Robbins v. Bd. of Trs. of Carbondale Police Pension Fund*, 177 Ill. 2d 533, 540 (1997). Most of the technologies listed under that definition (fingerprints, retina scans, and iris scans) are not "modern computing technologies"—they have existed for decades. *See* DB 10. The definition also *excludes* certain technologies that *are* "enhanced tools of measurement and analysis"—for example, "human biological samples used for valid scientific testing or screening." 740 ILCS 14/10. And most importantly, the term "biometric information" *also* contains the word "biometric," but it excludes information derived from photos. So whether or not BIPA "expresses the legislature's judgment that technologically enhanced identifiers require regulation" (PB 11), at least *some* such technologies were excluded from regulation—including Shutterfly's facial-recognition software.[3]

[3] Plaintiff's reading of the "photographs" exclusions also contradicts his own complaint. The crux of his argument is that "biometric identifier" and "biometric information" should be

B. Shutterfly's Technology Does Not Involve A "Scan Of Face Geometry" Because That Term Refers Only To An In-Person Scan.

We argued that even putting to one side BIPA's exclusion of photos and information derived from them, Shutterfly's technology does not involve a "scan of face geometry" because that term requires an in-person analysis. DB 6-7.

Plaintiff responds first that "[t]he definition of biometric identifiers . . . contains no reference whatsoever to the source of the identifier." PB 5; *see also Rivera*, 2017 WL 748590, at *5. Our argument, however, is not that BIPA has an *express* in-person requirement; it is that under a longstanding canon of construction (which plaintiff does not mention), the term "scan of face geometry" is narrowed in meaning by "its accompanying words," *Qualls*, 365 Ill. App. 3d at 1020, all of which describe in-person processes. DB 6-7.

Plaintiff contends next that because BIPA applies to private entities that "collect, capture, purchase, receive through trade, *or otherwise obtain* a . . . biometric identifier," the statute "clearly expresses the intent of the legislature to regulate biometric identifiers from any source, however obtained." PB 5, 10 (quoting 740 ILCS 14/15) (emphasis by plaintiff). But as plaintiff recognizes, this language is in BIPA's regulatory provision, not in its definition of biometric identifier, which is limited to data sources. By contrast, the definition of "biometric information" *does* make clear that the method of obtaining the data makes no difference: "any information, *regardless of how it is captured, converted, stored, or shared*, based on an

---

read differently precisely because the latter expressly excludes data derived from photos and the former does not. *See* PB 1, 8-9. But his complaint alleges that Shutterfly *also* collects "biometric information" by using "biometric identifiers . . . to identify individuals by name" and "to recognize their gender, age, race and location." Compl. ¶ 24. Plaintiff appears to recognize this tension, but halfheartedly defends his complaint's allegations in a footnote: "Because [gender, age, race, and location are] derived from 'biometric identifiers' as opposed to the photographs themselves, Shutterfly's unauthorized collection of this information also constitutes a violation of BIPA." PB 5 n.1. That makes no sense; if "biometric information" excludes data derived from photographs, then it clearly also excludes derivatives *of* those derivatives.

individual's biometric identifier used to identify an individual." 740 ILCS 14/10 (emphasis added); *see also People v. Goossens*, 39 N.E.3d 956, 959 (Ill. 2015) ("It is well settled that when the legislature uses certain language in one instance of a statute and different language in another part, we assume different meanings were intended."). This distinction again reflects the statute's meticulous structure: "Biometric identifier" is a short, well-defined list of original sources of data obtained from a person, and "biometric information" is (in plaintiff's words) a broader set of data derived from those sources, "however obtained, in person or otherwise." PB 10.

Finally, plaintiff argues that applying BIPA only to in-person scans would have negative "practical consequences" because each of the listed biometric identifiers "depends in the first instance on the capture of a photograph or, in the case of a voiceprint, an audio recording." PB 12. Not so. The scans listed in the definition of biometric identifier all involve the physical capture of information from the human body itself—an actual finger, an eye, spoken words, a hand, or a face—not from a photograph. *See* DB 7 & nn. 3-6. Although these live scans may produce an image that is then saved for later use, that image is instantaneously captured by a specialized recording device *as part of the scan itself.*[4] Shutterfly does not use a specialized device to conduct a live capture of the face; instead, a person takes an ordinary photo with an

[4] *See, e.g.*, Michael Zollhofer *et al.*, *Automatic Reconstruction of Personalized Avatars from 3D Face Scans*, COMPUTER ANIMATION AND VIRTUAL WORLDS 20 (2011), https://hal.archives-ouvertes.fr/hal-00631256/document (face scan involves "obtain[ing] a raw depth image of the face of a person sitting in front of" a device, resulting in "a high-quality 3D model of the scanned face"); Aleskey Golovinskiy *et al.*, *A Statistical Model for Synthesis of Detailed Facial Geometry*, 25(3) ACM TRANSACTIONS ON GRAPHICS (Proc. SIGGRAPH) 2-3 (July 2006), http://gfx.cs.princeton.edu/pubs/Golovinskiy_2006_ASM/facePaper.pdf ("Using a commercial 3D face scanner and a custom-built face scanning dome, we acquire high-resolution 3D face geometry. . . . Each subject sits in a chair with a head rest to keep the head still during acquisition."); Rein-Lien Hsu and Anil K. Jain, *Face Modeling for Recognition*, PROC. INT'L CONF. IMAGE PROCESSING 693 (2001), http://visgraph.cs.ust.hk/biometrics/Papers/Face/ICIP-2001A.pdf (describing "face" "scan" as a process for "modeling human faces/heads for facial animation," whereby "facial measurements are directly acquired from 3D digitizers or structured light range sensors").

ordinary camera and then uploads it to Shutterfly, often weeks or months later. That is far afield from what BIPA regulates.

C. BIPA Was Never Intended To Regulate Data Derived From Online Photos.

If BIPA's text left any doubt, the legislative findings and history confirm that it was not intended to regulate data derived from photos uploaded online. DB 8-9.

Legislative findings. BIPA's findings say repeatedly that the statute was designed to regulate the live use of biometric technologies in the narrow context of "financial transactions and security screenings." 740 ILCS 14/5(a); *see* DB 2, 8. Yet plaintiff proclaims, without any citation to the findings, that "the statute expresses a general intent to regulate and protect biometrics"; that "[t]he evil sought to be remedied by BIPA is private industry's presumptuous arrogation of the right to . . . create identifiers of private individuals"; and that "[t]he greatest evil" regulated by BIPA "occurs when privacy-invading operators like Shutterfly obtain an individual's picture and create a biometric identifier without his or her consent." PB 13-15 (internal quotation marks and citation omitted).

These assertions reflect the statute that plaintiff wants, not the one that was actually enacted. If the legislature had a "general intent to regulate and protect biometrics," it would not have defined its key terms using a short, exclusive list of items with express exclusions. If the "evil sought to be remedied" was *all* use of "biometrics," the legislature would have said so, rather than making statement after statement about financial transactions and security screenings.[5] And if the "greatest evil" targeted by the legislature was the application of

[5] *See* 740 ILCS 14/5(a) ("The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings."); *id.* 14/5(b) ("Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."); *id.* 14/5(c) ("[O]nce [biometrics are] compromised, the individual has no

facial-recognition technology to "an individual's picture," the legislature would not have *specifically excluded* photo-derived information from one of its two major definitions.

Plaintiff then argues that "[i]t would make no sense to safeguard biometrics *only* in [the financial and security] settings," because the "theft" of biometrics "is a security threat no matter how, when, or where it was stolen." PB 15. This policy opinion is plaintiff's, not the legislature's, and it is by no means the only sensible one. It was entirely reasonable for the legislature to conclude (as it did) that the "theft" of biometric data is worth regulating only "when such information is tied to finances" and security screenings (740 ILCS 14/5(d)), and that technology applied to photos does not create similar risks.

Legislative history. The General Assembly considered and *declined* to regulate *all* forms of "facial recognition" and all "records" of facial geometry; earlier versions of the statute were amended so that BIPA would regulate "scan[s] of . . . face geometry" and exclude data derived from photos. DB 8-9. Plaintiff attempts to brush off these amendments as "mere editorial revision[s]" designed to "refin[e] and streamlin[e] the statutory text." PB 16. He argues, for example, that "the term 'facial recognition' was unnecessary because a scan of face geometry *is* a form of 'facial recognition' technology." *Id.*; *see also Rivera*, 2017 WL 748590, at *8 ("For all the legislative history shows, the term was dropped simply because it was redundant with 'facial geometry.'"). But that response simply assumes the conclusion. The General Assembly obviously did *not* think that a scan of face geometry is the same thing as "facial recognition"; it

---

recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."); *id.* 14/5(e) ("Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.").

listed them separately in the earlier version of the bill, and then eventually decided not to include "facial recognition." That decision must be respected.[6]

II. BIPA DOES NOT AND CANNOT REGULATE THE OUT-OF-STATE CONDUCT ALLEGED IN THIS CASE.

Plaintiff's claim fails for the separate reason that Illinois has absolutely no interest in this lawsuit: (a) BIPA does not apply to out-of-state conduct and (b) any such application would violate the dormant Commerce Clause. DB 10-14.

A. Plaintiff Has Not Alleged A Sufficient Nexus To Illinois For BIPA To Apply.

Plaintiff recognizes that BIPA does not apply extraterritorially. PB 17 ("[T]he express provisions of BIPA evince no [extraterritorial] intent."); *see also Rivera*, 2017 WL 748590, at *9. He acknowledges that, accordingly, "only violations of BIPA that 'take place' inside Illinois are actionable," and that the BIPA "violation" alleged here is "Shutterfly's collection of Plaintiff's scans of face geometry without consent." PB 17-18. Most importantly, he concedes that "the Complaint[] *fail[s] to allege that Shutterfly actually extracts scans of face geometry from photographs in Illinois*." PB 19 (emphasis added). These concessions, combined with the fact that both parties reside outside Illinois, are dispositive of his claim. DB 10-11.

Nevertheless, plaintiff contends that a single allegation is sufficient to satisfy BIPA's extraterritoriality doctrine: "that an Illinois resident uploaded photographs of Plaintiff to Shutterfly's cloud-based service from within Illinois." PB 18 (citations omitted). He argues that "Shutterfly therefore could have obtained (but failed to obtain) the requisite written release from

[6] *See Gulf Oil Corp. v. Copp Paving Co.*, 419 U.S. 186, 200 (1974) (legislature's "delet[ion] [of] language . . . strongly militates against a judgment that [it] intended a result that it expressly declined to enact"); *Laborer's Int'l Union of N. Am., Local 1280 v. State Labor Relations Bd.*, 154 Ill. App. 3d 1045, 1050 (1987) ("[T]he intent of the state legislature can be derived not only from the language actually adopted, but also from the language which was changed or not adopted."); *Bergin v. Bd. of Trs. of Teachers' Ret. Sys.*, 31 Ill. 2d 566, 573 (1964) ("It is always proper to consider the course of legislation upon a particular statute . . . .").

Plaintiff *in Illinois*," because the uploader "could have provided to Shutterfly a statutorily compliant written release on Plaintiff's behalf" as his "legally authorized representative." *Id.* This theory has no basis in the complaint and is plainly insufficient to satisfy plaintiff's burden.

BIPA permits a "legally authorized representative" to provide the requisite written release for the use of a subject's biometric data. 740 ILCS 14/15(b)(3). But plaintiff's complaint does not allege that the unidentified uploader *was* his "legally authorized representative"—or even that the parties *communicated* before the upload. Nor does the complaint give any reason to believe that the uploader *could* have acted as plaintiff's "legally authorized representative"—a term ordinarily reserved for parents, guardians, or other individuals with legal authority to act for someone without the *capacity* to give consent.[7] Plaintiff's theory of liability would also have absurd results in practice: It would mean that if a user takes a selfie at Disney World and then uploads it to Shutterfly at O'Hare on his way home, BIPA would require Shutterfly to obtain the uploader's consent not only to analyze *his own* face, but also to analyze the faces of the innumerable *other* non-Illinois residents who happen to appear in the photo—on the theory that the user could have obtained a "written release" from those complete strangers as their "legally authorized representative." That cannot be right.[8]

---

[7] *See, e.g.*, 77 Ill. Admin. Code § 697.20 ("'Legally Authorized Representative' means an individual who is authorized to consent to HIV testing . . . for an individual who is: Under the age of 12, deceased, declared incompetent by a court of law, or otherwise not competent to consent . . . ."); *T.D. v. N.Y. State Office of Mental Health*, 626 N.Y.S.2d 1015, 1019 (1995) ("If a person lacks the capacity to consent . . . , consent may be obtained from the patient's legally authorized representative, defined in the regulations as the patient's spouse, parent, adult child, adult sibling, guardian or a committee of the person which is authorized to consent to [medical] research."); *Aponte v. United States*, 582 F. Supp. 65, 68 (D.P.R. 1984) ("'[L]egally authorized representative' means an individual, organization, or other judicially recognized body empowered under the applicable state law to act on behalf of a legally incompetent individual.").

[8] Due to an oversight, a similar hypothetical in our opening brief (DB 12) overlooked plaintiff's allegation that the uploader was residing in Illinois at the time of upload (*see* Compl.

Even if the location of the upload were a relevant Illinois connection, moreover, plaintiff has not come close to alleging that "the *majority* of circumstances relating to the alleged violation" of BIPA occurred in Illinois. *Landau*, 381 Ill. App. 3d at 65 (emphasis added). Illinois courts have routinely dismissed claims on extraterritoriality grounds even (1) when the *plaintiff* was an Illinois resident[9] and (2) when a "*scheme to defraud* was disseminated from a [defendant's] *headquarters*" in Illinois.[10] DB 11. It therefore cannot be the case that a *third party's* indisputably *lawful* conduct establishes an adequate state nexus.

Notably, although plaintiff relies heavily on *Rivera* in support of his interpretation of BIPA's provisions, he only briefly cites the court's analysis of Illinois' extraterritoriality requirement. *See* PB 20. The reason is obvious: it squarely supports our position on this issue. *Rivera* emphasized that "[t]he question" under the extraterritoriality doctrine "is whether

---

¶ 29). This allegation is immaterial, because only a *party's* residency can even arguably bear on the extraterritoriality analysis.

[9] *See, e.g.*, *Graham v. Gen. U.S. Grant Post No. 2665, V.F.W.*, 43 Ill. 2d 1, 2, 4 (1969) (plaintiff could not invoke the Illinois Dram Shop Act for injuries from a drunk-driving accident where "both the plaintiff and [the driver were] residents of Illinois" and the alcohol was sold in Illinois, because the "accident causing the plaintiff's injuries"—the event "[e]ssential to defendant's liability under the . . . Act"—"occurred in Wisconsin"); *Hackett v. BMW of N. Am., LLC*, 2011 WL 2647991, at *2 (N.D. Ill. June 30, 2011) (dismissing claim where plaintiff alleged that he was "an Illinois resident," that "he drove the vehicle in Illinois," and that he "experienced the [alleged fuel-pump] failure in Illinois," because he had "fail[ed] to show that the fraud occurred in Illinois"); *Valley Air*, 2009 WL 1033556, at *12 (Illinois statute did not apply because "the bulk of the circumstances making up the allegedly fraudulent transaction occurred" outside the state, even though plaintiff was "an Illinois citizen"); *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 775 (N.D. Ill. 2008) (Illinois residency insufficient absent "allegations that plausibly suggest that the purported deceptive domain scheme occurred primarily and substantially in Illinois"); *Walker v. S.W.I.F.T. SCRL*, 491 F. Supp. 2d 781, 795 (N.D. Ill. 2007) (dismissing claim where "the only connection to the state of Illinois is the fact that [one] plaintiff [was] a resident of Illinois").

[10] *See, e.g.*, *Avery*, 216 Ill. 2d at 189 ("The appellate court's conclusion that a scheme to defraud was 'disseminated' from State Farm's headquarters is insufficient."); *Philips*, 372 Ill. App. 3d at 58-59 ("The fact that a scheme to defraud was disseminated from a company's headquarters in Illinois is insufficient.").

Google's activities—making face templates of [plaintiffs] in photographs"—"are an extraterritorial (and therefore not-actionable) application of [BIPA]." 2017 WL 748590, at *10 (emphasis added). The court concluded that the complaint "*tip[ped] toward*" sufficiency because the plaintiffs had alleged *five* distinct Illinois connections: (1) that they were "Illinois residents"; (2) that their "photographs were taken in Illinois"; (3) that their "photographs were [ ] automatically uploaded in Illinois . . . from an Illinois-based [IP] address"; (4) that "Google failed to provide [plaintiffs] with required disclosures" in Illinois; and (5) that Google "failed to get [plaintiffs'] consent" in Illinois. *Id.* (emphasis added). Here, the complaint makes *only* the third of these allegations—and despite plaintiff's attempt to stretch that allegation beyond recognition, it has no relevance to BIPA or the conduct it regulates. If the *Rivera* complaint "tipped toward" sufficiency, the complaint here falls immovably on the other side of that line.[11]

B. Applying BIPA Here Would Violate The Dormant Commerce Clause.

The Constitution forbids the application of BIPA to these facts for two reasons: (1) it would have "the practical effect of . . . control[ling] conduct beyond the boundaries of [Illinois]"; and (2) it would create "inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another state." *Healy*, 491 U.S. at 336-37; DB 12-14.

On the first point, plaintiff responds that because "the photos were uploaded from within the state of Illinois and, therefore, [ ] Shutterfly could have obtained (but failed to obtain) a statutorily compliant written release for Plaintiff in Illinois[,] . . . the 'practical effects' of

[11] In the other cases plaintiff cites where the extraterritoriality doctrine was deemed satisfied (PB 18-20), the plaintiffs likewise alleged in-state residency *plus* several other Illinois connections to the statutory violation. *See Jamison v. Summer Infant (USA), Inc.*, 778 F. Supp. 2d 900, 910 (N.D. Ill. 2011) (plaintiff was a resident of Illinois, purchased the product at issue in Illinois, and used the product in Illinois, and the defendants "marketed and sold" the product in Illinois); *Gros v. Midland Credit Mgmt.*, 525 F. Supp. 2d 1019, 1024 (N.D. Ill. 2007) (in-state connections included "[plaintiff's] residence, the location of the alleged harm, . . . and the site of [plaintiff's] communications with [defendant]").

complying with BIPA are felt entirely in Illinois." PB 21. As just discussed, the location of the upload has nothing to do with Shutterfly's alleged failure to "comply" with BIPA. But even if it did, the effects of compliance would not be "*felt entirely* in Illinois." *Id.* (emphasis added). Again: Shutterfly is headquartered in California, and plaintiff has not alleged that *any component* of the facial-recognition process—the only conduct that BIPA is alleged to regulate—occurred in Illinois. *See, e.g.*, *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc) ("easily conclud[ing]" that a California statute violated the dormant Commerce Clause because it regulated sales that had "no necessary connection with the state other than the residency of the seller").

Plaintiff attempts to address the problems posed by inconsistent legislation in one sentence: "Shutterfly cites no legal authority, nor is there any, demonstrating that [BIPA] would result in Illinois projecting its regulatory policies into other states." PB 22. Shutterfly certainly did, and there certainly is. The opening brief cites three Seventh Circuit cases (ignored by plaintiff) that have taken "a broad[] view" of inconsistent state policies, under which even "the *absence* of a . . . counterpart" law in another state means that the other state "thinks [the conduct] shouldn't be restricted in the [same] way." DB 13 (emphasis added) (quoting *Midwest Title*, 593 F.3d at 667-68; citing *Morrison*, 649 F.3d at 538, and *Morley-Murphy*, 142 F.3d at 379). Here, Shutterfly has done more than show an "absence" of a similar law; California (where Shutterfly resides) has considered and *rejected* a statute that would have regulated "facial recognition technology." *Id.* Under Circuit law, Illinois cannot displace this deliberate policy choice or the decisions of the numerous other states that have declined to enact statutes like BIPA.[12]

[12] Oddly, plaintiff spends two pages of his brief addressing Shutterfly's "purported inability to refrain from collecting face scans only in Illinois." PB 21-22. That is a straw man: Our opening brief did *not* "assert[] that [Shutterfly] cannot comply with BIPA in Illinois" (PB 21); Shutterfly takes no position on this factual question at the pleading stage.

III. PLAINTIFF CANNOT RECOVER UNDER BIPA BECAUSE HE HAS NOT ALLEGED ACTUAL DAMAGES.

Plaintiff cannot recover statutory damages under BIPA because such damages are available only to those who have *suffered* actual damages but cannot prove their full *amount*—and he does not seek or allege such damages here. DB 14-15. Plaintiff offers two responses.

First, he argues that because "BIPA entitles an aggrieved party to recover liquidated damages '*or*' statutory damages," it allows "a binary election between actual or statutory liquidated damages." PB 23 (emphasis added). According to plaintiff, this language distinguishes BIPA from the statutes at issue in *Sterk* and *Doe*, which did not use the word "or." *See Sterk*, 672 F.3d at 537 (statute allowed "actual damages but not less than liquidated damages in an amount of $2,500"); *Doe*, 540 U.S. at 619 (statute permitted "actual damages sustained . . . , but in no case [could] a person entitled to recovery receive less than . . . $1,000").

That distinction, however, is meaningless. Like BIPA, the statutes in *Sterk* and *Doe* did not *expressly* require proof of actual damages. *See, e.g.*, *Sterk*, 672 F.3d at 538 (interpreting the statute to "allow[] $2,500 in liquidated damages, *without need to prove actual damages*" (emphasis added) (internal quotation marks omitted)). But because "liquidated damages . . . *must* be a reasonable attempt to estimate actual damages," *Pace*, 31 F.3d at 593 (emphasis added), both courts held that this requirement was properly incorporated into the statute's *liquidated* damages provision. As *Sterk* explains, "liquidated damages are intended to be an estimate of actual damages," and if a statutory violations "results in no injury at all," "the only possible estimate of actual damages . . . would be zero." 672 F.3d at 538 (citing *Pace* and *Doe*); *see also M.I.G. Invs., Inc. v. Marsala*, 92 Ill. App. 3d 400, 405 (1981) ("A liquidated damages clause will be given effect if actual damages are difficult to ascertain and a liquidated damages provision is a reasonable estimate of [actual] damages."). The same is true of BIPA, as two

courts have held. *McCollough*, 2016 WL 4077108, at *4; *Rottner* (Ex. F to DB). Contrary to plaintiff's suggestion (PB 23 n.8), neither *Rivera* nor *Norberg* was faced with this question.

Second, in several final pages of howling rhetoric, plaintiff contends that he "has suffered actual damages" because Shutterfly supposedly subjected him to an "egregious [ ] violation of personal privacy . . . for the self-evident purpose of building a comprehensive database of individuals' immutable biometric identities, enhancing the power of its services in the eyes of users, and thus the formidability of its brand." PB 23-24. This argument can be disregarded because plaintiff's *complaint* does not claim that he suffered these damages. Plaintiff's *ad hominem* attack on Shutterfly's motivations—judged solely from its creation of a free tool that helps people organize and share photos of their friends and loved ones—is not only far from "self-evident"; it is entirely unwarranted.

CONCLUSION

The Court should dismiss the complaint with prejudice.

Date: May 12, 2017

By: /s/ *Lauren R. Goldman*

Lauren R. Goldman
Michael Rayfield (*pro hac vice*)
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco (*pro hac vice*)
MAYER BROWN LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

Counsel for Defendant Shutterfly, Inc.